Trust Data Protection – Data Sharing Guidance V1.1

To ensure that the sharing of Trust and school level data complies with the law the checklists below should be used in conjunction with the following policies and guidance:-

- Trust Data Protection and Freedom of Information Policy
- Trust Data Protection Training
- Staff Privacy Notice
- Student Privacy Notice
- ICO Data Sharing Code of Practice - https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

Please forward Data Protection requests to the School Business Manager. Advice is available from the Trust Compliance Officer for complex requests.

<table>
<tr><th colspan="2">DATA SHARING CHECKLISTS</th></tr>
<tr><th>ONE OFF REQUESTS</th><th>SYSTEMATIC DATA SHARING</th></tr>
<tr>
<td>
Example: You are asked to share personal data relating to a pupil, family members or member of staff in a ‘one off’ circumstance e.g. a parent asks for a copy of their child’s education records or the school receives a request for data in relation to a criminal investigation.

<u>KEY POINTS TO CONSIDER</u>

IS THE SHARING JUSTIFIED?
• Do you think you should share the information?
• Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing? (e.g. SEN data/Child Protection details)
• Have you assessed the potential benefits and risk to individuals and/or society of sharing or not sharing?
• Do you have concerns that an individual is at risk of serious harm?
• Do you need to consider an exemption in the DPA to share?

DO YOU HAVE THE POWER TO SHARE?
• Is the data outlined in the Student/Staff Privacy Notices and has consent been obtained?
• The nature of the information you have been asked to share (for example was it given in confidence. E.g. Child Protection details – involved the school DSL).
• Any legal obligation to share information (for example a statutory requirement or a court order e.g. Police Section 29 Request or Education Act – The law allows the transfer of pupil data when a child moves schools and to other agencies (as per Privacy Notice).

IF YOU DECIDE TO SHARE
What information should you share?
</td>
<td>
Example: You want to enter into an agreement to share staff or student personal data on an ongoing basis e.g. MIS Systems and systems//web platforms and apps which link to school MIS Systems or require manual uploads of staff and student data. A Data Protection Impact Assessment (DPIA) needs to be completed – see School Business Manager or IT Network Manager in first instance.

KEY POINTS TO CONSIDER

IS THE SHARING JUSTIFIED?
• What is the sharing meant to achieve?
• Have you assessed the potential benefits and risk to individuals and/or society of sharing or not sharing?
• Is the sharing proportionate to the issue you are addressing?
• Could the objective be achieved without sharing personal data?

DO YOU HAVE THE POWER TO SHARE?
Requests for systems to be linked to school pupil and staff data should be requested through the School Business Manager who can liaise with the school ICT lead and system supplier to ensure data protection security protocols are adequate.

IF YOU DECIDE TO SHARE
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

• The organisations that will be involved.
• What you need to tell people about the data sharing and how you will communicate that information.
</td>
</tr>
</table>

- Only share what is necessary – e.g. redact information if it does not relate directly to individual named in the data request (data subject).
- Distinguish fact from fiction.

How should the information be shared?

- Information must be shared securely e.g. encrypted document/email or via www.gov.uk Secure Access S2S School transfer or BSO Dropbox. Seek advice if you are unsure.
- Ensure you are giving the data to the right person – always check the identity and source of requests.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record the decision

All requests and decisions should be recorded on the school Data Protection Register as per the Trust Data Protection and Freedom of Information Policy.

- Measures to ensure that adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Many reputable systems suppliers will incorporate a Data Sharing Protocol as part of their agreement; schools should make sure this is adequate.

Record the Data Sharing Agreement/Data Protection Impact Assessment

Copy Data Sharing Agreements/DPIAs should be stored with the contract paperwork.

TAKE CARE WHEN DEALING WITH STUDENT AND STAFF DATA

Personal data is an individual's name and any other piece of identifying information – see below for examples of personal data handled in schools.

- Address details
- SEN status
- Free School Meals eligibility
- Pupil Premium
- Educational levels and results (Inc. mock/practice exam papers/pieces of work with comments/feedback)
- Child Protection details
- Witness/Incident details
- Accident Records
- Photographs
- Staff Payroll/Salary information
- Staff Performance Management details

TOP TIPS TO KEEP DATA SAFE

- Documents containing personal data should be shredded or placed in Security Waste Consoles.
- Do not leave documents printing which contain personal data – see above for examples.
- If something personal is left on a printer or somewhere public, pass it to the School Business Manager.
- Take care when using electronic whiteboards in classrooms - registers often show FSM, SEN alerts etc.
- Parent evenings etc. take care not to inadvertently display other student's results/grades if using lists.
- Ensure you confirm the identity of callers and email addresses before discussing personal data.
- Where necessary to send data elsewhere, send it securely – see Data Protection Training for guidance.
- Keep your working area and desk tidy and do not leave documents lying around for others to see.
- Take care not to display personal data if visitors and students regularly use your office.
- Lock your PC/Laptop when not in use – especially in classrooms/public areas.
- Check the school holds signed Privacy Notices before sharing any data covered by the Privacy Notices.